

## CLAIMS

What is claimed is:

- 1 1. A computer-implemented method comprising:  
2 receiving a request to generate a secure electronic record of a third-party transaction,  
3 wherein the received request includes data associated with the third-party transaction;  
4 generating the secure electronic record of the third-party transaction; and  
5 transmitting at least a portion of the secure electronic record to a client system.
- 1 2. The method of claim 1, wherein generating the secure electronic record of the third-  
2 party transaction comprises:  
3 generating a hidden part of the secure electronic record to be accessible by at least a  
4 subset of a plurality of clients; and  
5 generating a visible part of the secure electronic record to be accessible by at least a  
6 subset of the plurality of clients.
- 1 3. The method of claim 1, wherein generating the secure electronic record of the third-  
2 party transaction comprises:  
3 authenticating the received data associated with the third-party transaction.
- 1 4. The method of claim 1, wherein generating the secure electronic record of the third-  
2 party transaction comprises:  
3 generating a digital signature for the secure electronic record.
- 1 5. The method of claim 1, wherein generating the secure electronic record of the third-  
2 party transaction comprises:  
3 encrypting at least a portion of the secure electronic record.

1 6. The method of claim 1, wherein generating the secure electronic record of the third-  
2 party transaction comprises:  
3 providing an identifier for the secure electronic record to uniquely identify the secure  
4 electronic record.

1 7. The method of claim 1, wherein generating the secure electronic record of the third-  
2 party transaction comprises:  
3 generating a secure electronic receipt of the third-party transaction

1 8. The method of claim 1, wherein receiving data associated with the third-party  
2 transaction further comprises:  
3 receiving data associated with the third-party transaction from a first client system;  
4 and  
5 receiving data associated with the third-party transaction from a second client system,  
6 wherein the second client system receives at least a portion of the data associated with the  
7 third-party transaction from the first client system.

1 9. The method of claim 1, wherein receiving data associated with the third-party  
2 transaction comprises:  
3 receiving an authentication token corresponding to the data associated with the third-  
4 party transaction.

1 10. The method of claim 1, wherein receiving data associated with the third-party  
2 transaction comprises:  
3 receiving a digital signature corresponding to the data associated with the third-party  
4 transaction.

1 11. The method of claim 1, wherein the secure electronic record is a secure electronic  
2 receipt.

1 12. The method of claim 11, wherein receiving data associated with the third-party  
2 transaction comprises:  
3 receiving the data according to the HyperText Transfer Protocol (HTTP).

1 13. The method of claim 1, wherein transmitting at least a portion of the secure electronic  
2 record to a client further comprises:  
3 transmitting a first portion of the secure electronic record to a first client; and  
4 transmitting a second portion of the secure electronic record to a second client.

1 14. The method of claim 1, wherein transmitting at least a portion of the secure electronic  
2 record to a client comprises:  
3 transmitting at least a portion of the secure electronic record to a special authority.

1 15. The method of claim 14, wherein the special authority is a tax collecting authority.

1 16. The method of claim 1, wherein the received request specifies at least some of a  
2 plurality of clients to which the secure electronic record is transmitted.

1 17. The method of claim 1, wherein the received request defines a portion of the secure  
2 electronic record that is transmitted to the client.

1 18. The method of claim 1, further comprising:  
2 encrypting, at least a portion of, the generated secure electronic record of the third-  
3 party transaction.

- 1 19. The method of claim 1, further comprising:  
2 obtaining a digital signature corresponding to the received data associated with the  
3 third-party transaction.
- 1 20. The method of claim 1, further comprising:  
2 authenticating the received data associated with the third-party transaction.
- 1 21. The method of claim 1, wherein the client is a special authority client system.
- 1 22. The method of claim 21, wherein the special authority client system is a tax collecting  
2 authority client system.
- 1 23. The method of claim 1, further comprising:  
2 maintaining a copy of the transmitted portion of the secure electronic record to  
3 validate the transfer of the secure electronic record.
- 1 24. A system comprising:  
2 a secure electronic record server system to generate a secure electronic record  
3 responsive to receiving data associated with a third-party transaction; and  
4 a plurality of client systems coupled with the server system to receive the secure  
5 electronic record from the secure electronic record server system.
- 1 25. The system of claim 24, wherein the plurality of client systems includes a tax  
2 collecting authority client system.

1 26. The system of claim 24, wherein the secure electronic record is a secure electronic  
2 receipt.

1 27. The system of claim 24, wherein the secure electronic record server system is coupled  
2 with the plurality of client systems through the Internet.

1 28. The system of claim 27, wherein the secure electronic record server system  
2 comprises:  
3 an authentication mechanism to authenticate the received data associated with the  
4 third-party transaction.

1 29. The system of claim 28, wherein the authentication mechanism implements, at least  
2 in part, Request For Comments 2617 to authenticate the received data associated with the  
3 third-party transaction.

1 30. The system of claim 27, wherein the secure electronic record server system  
2 comprises:  
3 an encryption mechanism to encrypt at least a portion of the secure electronic record.

1 31. The system of claim 30, wherein the encryption mechanism implements, at least in  
2 part, the Extensible Markup Language Encryption Standard to encrypt at least a portion of  
3 the secure electronic record.

1 32. The system of claim 27, wherein the secure electronic record server system  
2 comprises:  
3 a digital signature mechanism to verify that the received data associated with the  
4 third-party transaction has not been altered.

1 33. The system of claim 32, wherein the digital signature mechanism implements, at least  
2 in part, Request For Comments 3275 to verify that the received data associated with the  
3 third-party transaction has not been altered.

1 34. The system of claim 24, wherein the secure electronic record server system  
2 comprises:  
3 an identifier generator to provide a unique identifier for the secure electronic record.

1 35. An application server comprising:  
2 a network interface to connect to a client system;  
3 a processor and logic executable thereon to  
4 receive a request to generate a secure electronic record of a third-party  
5 transaction from the client system, wherein the received request includes data  
6 associated with the third-party transaction,  
7 generate a secure electronic record of the third-party transaction, and  
8 transmit at least a portion of the secure electronic record to a plurality of  
9 clients; and  
10 a network interface to connect to at least one of the plurality of clients.

1 36. The application server of claim 35, wherein the processor and logic executable  
2 thereon to generate the secure electronic record of the third-party transaction at the server  
3 system includes logic executable thereon to:  
4 authenticate the received data associated with the third-party transaction.

1 37. The application server of claim 35, wherein the processor and logic executable  
2 thereon to generate the secure electronic record of the transaction at the server system  
3 includes logic executable thereon to:  
4 reference a digital signature associated with the received data to determine whether  
5 the received data has been altered.

1 38. The application server of claim 35, wherein the processor and logic executable  
2 thereon to generate the secure electronic record of the transaction at the server system  
3 includes logic executable thereon to:  
4 encrypt at least a portion of the secure electronic record.

1 39. The application server of claim 35, further comprising:  
2 an identifier generator to provide a unique identifier for the secure electronic record.

1 40. An application server comprising:  
2 means for receiving a request to generate a secure electronic record of a third-party  
3 transaction, wherein the received request includes data associated with the third-party  
4 transaction;  
5 means for generating the secure electronic record of the third-party transaction; and  
6 means for transmitting at least a portion of the secure electronic record to a plurality  
7 of client systems.

1 41. The system of claim 40, wherein the means for generating the secure electronic  
2 record of the third-party transaction comprises:  
3 means for generating a hidden part of the secure electronic record to be accessible by  
4 a subset of the plurality of clients; and

5 means for generating a visible part of the secure electronic record to be accessible by  
6 the plurality of clients.

1 42. The system of claim 40, wherein the means for generating the secure electronic  
2 record of the transaction at the server system comprises:

3 means for authenticating the received data associated with the transaction.

1 43. The system of claim 40, wherein the means for generating the secure electronic  
2 record of the third-party transaction comprises:

3 means for creating a digital signature associated with the generated secure electronic  
4 record to provide an indication of whether the generated secure electronic record has been  
5 altered.

1 44. The system of claim 40, wherein the means for generating the secure electronic  
2 record of the third-party transaction comprises:

3 means for encrypting at least a portion of the secure electronic record.

1 45. The system of claim 40, wherein the means for generating the secure electronic  
2 record of the third-party transaction comprises:

3 means for providing an identifier for the secure electronic record to uniquely identify  
4 the secure electronic record.

1 46. The system of claim 40, wherein the means for generating the secure electronic  
2 record of the third-party transaction comprises:

3 means for generating a secure electronic receipt for the third-party transaction.

1 47. An article of manufacture comprising:



2 an electronically accessible medium providing instructions that, when executed by an  
3 apparatus, cause the apparatus to  
4 receive a request to generate a secure electronic record of a third-party transaction,  
5 wherein the received request includes data associated with the third-party transaction;  
6 generate the secure electronic record of the third-party transaction; and  
7 transmit at least a portion of the secure electronic record to a plurality of clients.

1 48. The article of manufacture of claim 47, wherein the electronically accessible medium  
2 provides further instructions that, when executed by the apparatus, cause the apparatus to  
3 encrypt the generated secure electronic record of the third-party transaction.

1 49. The article of manufacture of claim 47, wherein the electronically accessible medium  
2 provides further instructions that, when executed by the apparatus, cause the apparatus to  
3 obtain an electronic signature corresponding to the received data associated with the  
4 third-party transaction.

1 50. The article of manufacture of claim 47, wherein the electronically accessible medium  
2 provides further instructions that, when executed by the apparatus, cause the apparatus to  
3 authenticate the received data associated with the third-party transaction